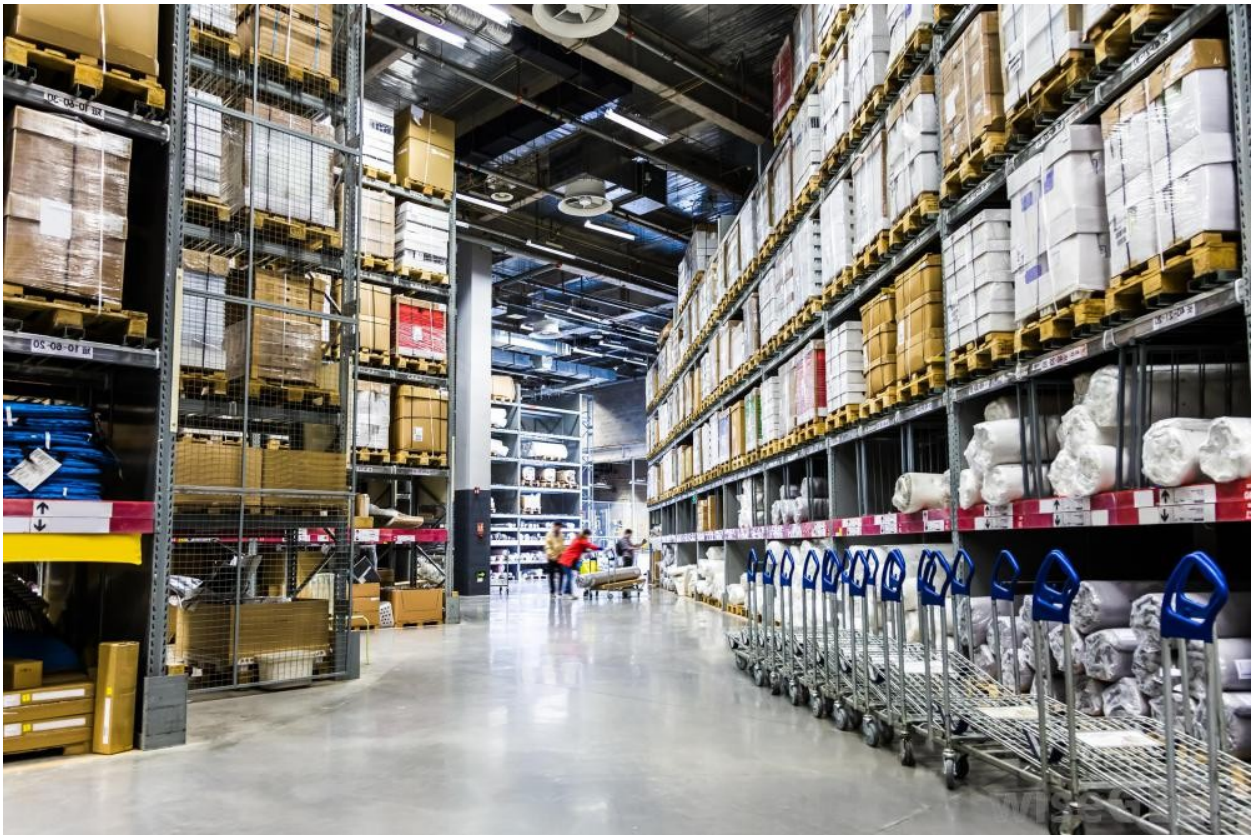


Large Box Store Retail Tabletop Exercise

Situation Manual

[Insert Date]

[Insert Caveat]

Photo Courtesy of WiseGeek

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

Exercise Agenda

Start Time	End Time	Activity
7:45 a.m.	8:30 a.m.	Registration
8:30 a.m.	8:45 a.m.	Welcome and Introductions
8:45 a.m.	9:45 a.m.	Module One: Intelligence and Information Sharing
9:45 a.m.	9:55 a.m.	Break
9:55 a.m.	10:55 a.m.	Module Two: Incident and Response
10:55 a.m.	11:05 a.m.	Break
11:05 am.	12:05 p.m.	Module Three: Business Continuity and Recovery
12:05 p.m.	12:30 p.m.	Hot Wash

**All times are approximate*

This page is intentionally left blank.

EXERCISE OVERVIEW

Exercise Name	Large Box Store Retail Tabletop Exercise (TTX)
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a TTX, planned for [insert exercise duration], and will focus on [insert scope]. This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP).
Mission Area(s)	Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Areas]
Capabilities	Planning; Public Information and Warning; Operational Coordination; Intelligence and Information Sharing; Interdiction and Disruption; On-Scene Security, Protection, and Law Enforcement; Economic Recovery; and Health and Social Services; [insert other core capabilities]
Objectives	1. Review pre-incident and incident response information sharing procedures between corporate leadership, employees, customers, and emergency responders. 2. Discuss private sector stakeholders' emergency preparedness plans and response procedures to an Active Shooter / Improvised Explosive Device (IED) incident and the coordination of activities under National Incident Management System (NIMS) with local, state, and federal agencies. 3. Consider participating organizations' business continuity plans or continuity of operations plans to identify best practices in the aftermath of a complex coordinated attack on a large box store. 4. [Insert additional exercise objectives as necessary]
Threat or Hazard	Active Shooter and IED

Scenario	An interactive, discussion-based exercise focused on an Active Shooter / IED incident threatening a large box store. The scenario consists of three modules: Intelligence and Information Sharing; Incident and Response; and Business Continuity and Recovery.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]
Participating Organizations	[Please see Appendix B.]
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor).]

General Information

Exercise Objectives and Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

Exercise Objectives	Capability
Review pre-incident and incident response information sharing procedures between corporate leadership, employees, customers, and emergency responders.	✓ Planning ✓ Intelligence and Information Sharing ✓ Public Information and Warning
Discuss private sector stakeholders' emergency preparedness plans and response procedures to an Active Shooter / IED incident and the coordination of activities under NIMS with local, state, and federal agencies.	✓ Planning ✓ Operational Coordination ✓ Interdiction and Disruption ✓ On-Scene Security, Protection, and Law Enforcement
Consider participating organizations' business continuity plans or continuity of operations plans to identify best practices in the aftermath of a complex coordinated attack on a large box store.	✓ Planning ✓ Economic Recovery ✓ Health and Social Services
[Insert objective]	✓ [Insert capability aligned to each objective]

Table 1. Exercise Objectives and Associated Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers:** Do not directly participate in the exercise. However, they may support the development of player responses to the situation

during the discussion by asking relevant questions or providing subject matter expertise.

- **Facilitator:** Provides situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
- **Evaluators:** Are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

- Module One: Intelligence and Information Sharing
- Module Two: Incident and Response
- Module Three: Business Continuity and Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

Exercise Guidelines

- This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your jurisdiction's/ organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.

- The assumption is that the exercise scenario is plausible and events occur as they are presented. All players will receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

Module One: Intelligence and Information Sharing

Scenario

[Insert Month, Day, Year]: [Time]

Based on recent intelligence gathering efforts, the Secretary of Homeland Security, in coordination with other federal entities, issued an "Elevated" Threat Alert through the National Terrorism Advisory System (NTAS) warning of a credible terrorist threat against the U.S. At this time, there is no specific information which would warrant the release of an "Imminent" Threat Alert.

The details of the alert state that the threat it from domestic anti-corporate terrorist groups in the U.S. with ties to international terrorist organizations, which are focused on large box stores. The alert is to remain in place until [Insert Date + 3 months].

The [Insert relevant State or local agency], using [insert state / regional fusion center], has passed on the alert to its partners in the Commercial Facilities Sector.

Additional information about the alert can be found in **Appendix A**.

Discussion Questions

1. How would your agency or organization expect to receive information about a credible threat?
    a. What steps does your agency or organization take once they receive notice of a credible threat?
2. Does your agency or organization receive NTAS alerts?
    a. Does your agency or organization receive Suspicious Activity Bulletins?

3. Does your organization maintain a relationship with your CISA Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
4. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
5. What internal information sharing and dissemination processes does your organization currently have in place?
6. What information or warnings about the elevated threat level are being released to the public?
    a. Who is responsible for the initial messaging?
    b. How quickly is information being released?
    c. What methods are being used to distribute information?
    d. What should the content of the messaging be?
    e. Are businesses or other organizations providing their own messaging to their employees?
    f. How are messages coordinated across the different agencies and organizations?
7. Would you share this threat information with international industry partners? What would be the benefit, if any?
8. Are there technological barriers, policies, legal considerations, or institutional sensitivities that might affect information sharing?
9. Does your agency or organization conduct any specific training based on credible threats?
10. What risk mitigation or protective actions would you implement?
    a. Would you take any additional measures to monitor for suspicious activities?

Module Two: Incident and Response

Scenario

[Insert Date + 7 Days]: [Time]

At approximately [insert time], two individuals drive into the [Insert Name] parking lot in a white van and park near the entrance of [Insert Name]. One man exits from the driver's seat carrying a large backpack, while the second comes out of the van's back door a few moments later holding a duffel bag. The two enter the large box store and begin walking towards the public restrooms.

As the men move towards the restrooms, a customer in the immediate vicinity becomes suspicious and alerts a nearby store employee. When the guard approaches the two, the backpack carrying individual removes a handgun and fires it, wounding the guard. Upon hearing gunfire, customers in the area begin panicking, running towards the secondary exits and hiding behind any shelter they can find as they begin desperately contacting 911 dispatch.

After encountering the security guard, the two men remove additional firearms from their respective bags and work their way through the store, firing indiscriminately at customers and store employees alike.

Discussion Questions

1. What actions would you take at this time?
    a. What resources and assets do you have available to assist in the response?
2. Are there protocols in place at the store to alert customers / employees of an emergency? Who is responsible for enacting them?
3. What are crowd control and / or evacuation procedures for an event of this type?
    a. Who is responsible for activating the evacuation procedures?
    b. Is there a specific location for evacuees?
        i. Are there secondary and tertiary rally points in case the primary rally point is a part of the incident or overwhelmed by evacuees?
4. Would there be any accountability of the employees in the store and, if so, how is this accomplished?
5. Is there security staff on-site? How are they trained to respond to active shooter incidents?

   a. Is there local law enforcement onsite?

6. How will local law enforcement respond to this incident?
   a. What steps must be taken prior to engaging the shooters?
   b. In addition to responding to the threat, what other services would they be expected or asked to provide?
   c. What other emergency services would respond to this incident?
7. What additional local response assets are available to be requested? What would their response time be?
8. At this point in the response, are there any messages being released to the public?
   a. Who is responsible for this type of messaging?
   b. How is this messaging coordinated?
9. At this point in the response, would you share information with the larger community? How? When?
   a. Who is responsible for this type of messaging?
   b. What would other organizations do with this information?
   c. Would other organizations assist you in your response? Are there any Memorandums of Understanding in place?
   d. How would local law enforcement share information with the community?
10. What measures will be taken to streamline the information sharing process?
   a. How will you resolve potential misinformation?
   b. How will you respond to and coordinate any requests for comment by the media?

Scenario Update

Date: [Insert Same as Above]
Time: [Incident + 20 Minutes]

Customers and employees that have either fled the scene or are still trapped in the store continue to call the local 911 dispatch. According to callers inside the facility, the gunmen are walking down the shopping aisles wielding assault rifle-styled weaponry and shooting at anyone they find. Callers report several wounded bystanders, including multiple people lying motionless on the ground.

As law enforcement arrives and initiates entry into the building, an explosion erupts from inside the shooters' van in front of the store, devastating several adjacent parked cars and damaging nearby response vehicles. Outside callers and local response agencies, via radio communications, report the detonation. In response to this newly received information, additional police, fire, and Emergency Medical Service (EMS) units are requested, along with bomb detection and disposal agencies.

Discussion Questions

1. What procedures, if any, do law enforcement, fire, and EMS agencies have in place to respond to an attack on their own personnel?
2. If incident command staff are killed or injured, who takes command?
    a. Is this process well known and exercised?
    b. About how long would it take to re-establish a working command post?
    c. What procedures would be considered to ensure the safety of first responders and command staff?
    d. What additional security procedures to ensure responders' safety would be considered that would suspend or slow life-saving operations until fully implemented?
3. What is the standard operating procedure after law enforcement officers encounter IEDs in this situation?
    a. Will additional response, predominantly when engaging the active shooters, be delayed?
4. How would law enforcement re-establish the surrounding area as secure?
    a. What steps need to take place to ensure the area is cleared of all potential threats?

   b. Would these actions be concurrent or take place after entry of the building?

5. What impact does the expanding incident area have on the command structure?
6. Would there be sufficient resources immediately available for both incidents?
7. What information, if any, would be passed on to the public? Who is responsible for this messaging?
8. At what point would federal agencies, such as the Federal Bureau of Investigation (FBI) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) be contacted?
9. Do your agencies or organizations cross-train on complex coordinated attack scenarios?

Scenario Update

Date: [Insert Same as Above]
Time: [Insert Time + 40 Minutes]

After securing the outside perimeter with bomb detection and disposal units, law enforcement officers enter [Insert Name]. Units report at least [insert number] confirmed fatalities, as well as approximately [insert number] victims with injuries varying in severity.

The officers continue through the store and encounter the two gunmen in a main aisle. They engage the pair, neutralizing them both.

Discussion Questions

1. Who is responsible for securing the scene?
    a. Would this differ regarding the exterior parking lot and the interior box store?
2. What steps need to take place to ensure the building is cleared of all gunmen and potential IEDs?
3. What protocols are in place to allow fire and EMS personnel to make entry into the store when assisting injured customers and casualties?
4. What procedures are taken to stand up an emergency operations center (EOC)?
    a. What level of activation do you anticipate for this incident?
    b. What are the communication procedures for the different levels?
5. Would incident command establish a joint information center (JIC)?
    a. If so, who would be included in the JIC?
6. How are hospitals notified about the number and severity of the wounded?
    a. What procedures are in place to handle a mass casualty incident?
7. Would mass care facilities, family assistance, or reunification centers be set up?
    a. What procedures are in place?
    b. Which agency or organization would be in charge?
8. Who is responsible for communicating information to family members of those killed or injured?

This page is intentionally left blank.

Module Three: Business Continuity and Recovery

Scenario

[Insert Date + 3 Days]: [Time]

Three days have passed since the attack on [Insert Name], and the investigation is still underway. A distinct motive for selecting [Insert Name] is not evident, although ties between the deceased gunmen and domestic anti-corporate terrorist groups have been identified.

There were a total of [insert number] fatalities resulting from the shooting and IED incident, with an additional [insert number] victims that sustained various injuries resulting from the ensuing panic; [insert number] of these were life threatening. Those [insert number], along with [insert number] others, are still hospitalized at the present time.

Local and federal authorities have gathered all evidence from the large box store parking lot and have turned security of the vicinity back over to [Insert Name] ownership, who subsequently begin cleanup and recovery operations.

Discussion Questions

1. How will the ramifications of such an event be addressed regarding the business continuity planning or rapid recovery operations?
    a. Does your organization have a continuity of operations plan or business continuity plan in place?
    b. What are the implications of being unable to open your retail store to the public for a period of time?
    c. Is your organization able to relocate to another facility? If so, how long would this take?
    d. How would the loss of personnel impact your operations? What steps would be taken to adjust for or mitigate these losses?
    e. How is information communicated with personnel and families during the days following the incident?
    f. Will owners / operators face liability issues from the attack?
2. How will government organizations continue to manage response efforts while beginning long-term recovery processes?
    a. How will employee absences (because of personal / family impacts from the incident) affect response and recovery efforts?

b. What state and / or federal resources would your organization request? What state and / or federal assistance would your organization require?

c. What aid would your organization provide to private sector assets or resources?

   i. How are roles and responsibilities delineated?

   ii. What plans or programs outline this aid or assistance?

d. What private sector assets or resources are available to assist your organization and the overall response effort?

   i. Are pre-arranged agreements in place with private sector organizations to provide resources?

   ii. If so, how are these agreements activated (i.e., what type of coordination and information sharing is required)?

   iii. How will this coordination and information sharing take place?

e. What non-traditional resources does your organization have access to?

3. How will patron and employee personal item loss, including motor vehicles damaged in the IED explosion, be addressed?

4. Given the scenario, what measures would be needed to support your organization's employees following this event?

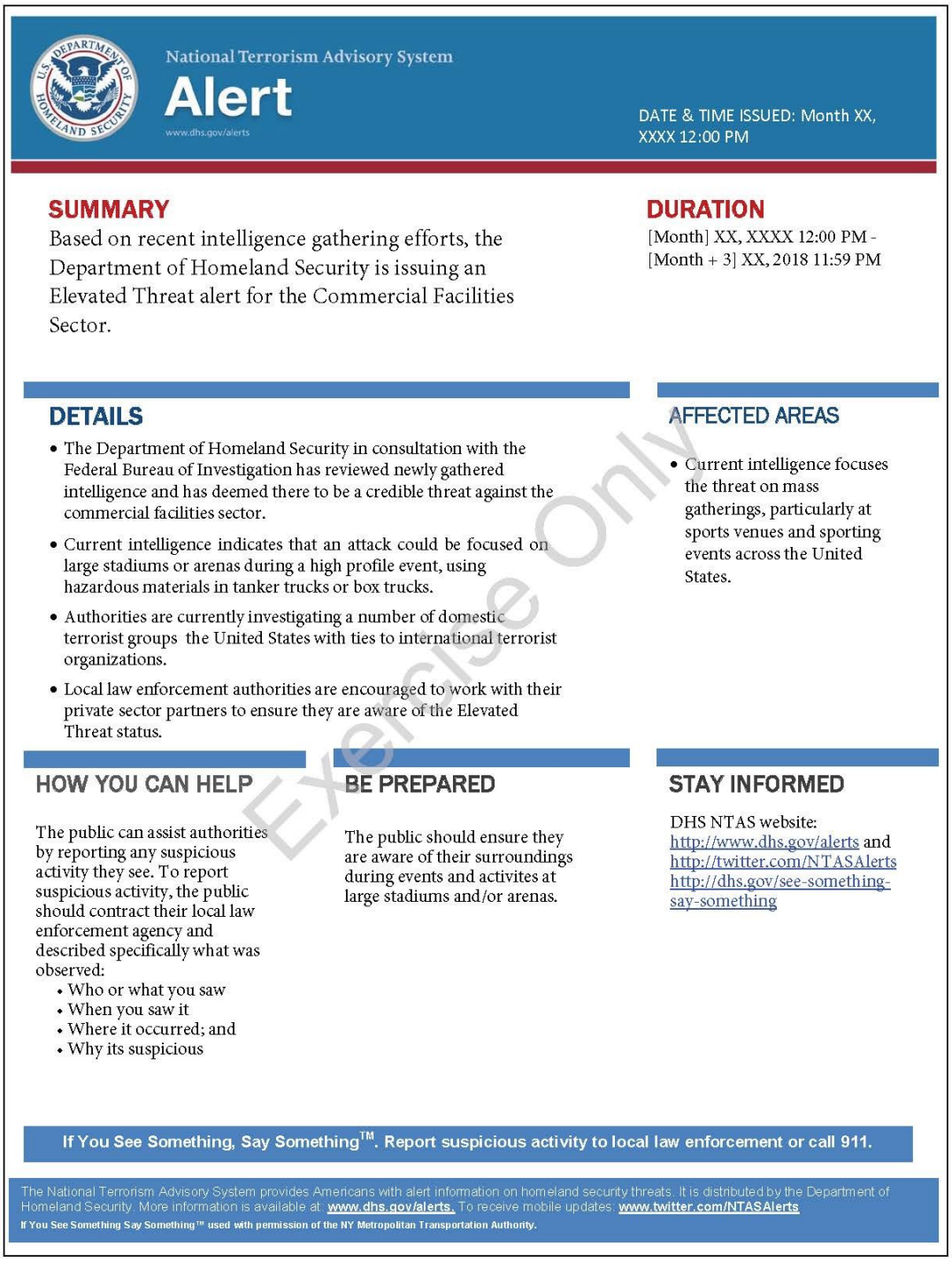
   a. How is information communicated to employees during the days and weeks following the incident?

   b. Will mental health counseling for employees and family members be available?

   c. Is financial assistance available to employees if operations are suspended for an extended length of time?

5. At what point would you consider the impacted area and all associated organizations or businesses stabilized and back to steady state?

APPENDIX A: SAMPLE NATIONAL TERRORISM ADVISORY SYSTEM ALERT



National Terrorism Advisory System

Alert

www.dhs.gov/alerts

DATE & TIME ISSUED: Month XX, XXXX 12:00 PM

SUMMARY

Based on recent intelligence gathering efforts, the Department of Homeland Security is issuing an Elevated Threat alert for the Commercial Facilities Sector.

DURATION

[Month] XX, XXXX 12:00 PM - [Month + 3] XX, 2018 11:59 PM

DETAILS

- The Department of Homeland Security in consultation with the Federal Bureau of Investigation has reviewed newly gathered intelligence and has deemed there to be a credible threat against the commercial facilities sector.
- Current intelligence indicates that an attack could be focused on large stadiums or arenas during a high profile event, using hazardous materials in tanker trucks or box trucks.
- Authorities are currently investigating a number of domestic terrorist groups the United States with ties to international terrorist organizations.
- Local law enforcement authorities are encouraged to work with their private sector partners to ensure they are aware of the Elevated Threat status.

AFFECTED AREAS

- Current intelligence focuses the threat on mass gatherings, particularly at sports venues and sporting events across the United States.

HOW YOU CAN HELP

The public can assist authorities by reporting any suspicious activity they see. To report suspicious activity, the public should contract their local law enforcement agency and described specifically what was observed:

- Who or what you saw
- When you saw it
- Where it occurred; and
- Why its suspicious

BE PREPARED

The public should ensure they are aware of their surroundings during events and activites at large stadiums and/or arenas.

STAY INFORMED

DHS NTAS website:
http://www.dhs.gov/alerts and
http://twitter.com/NTASAlerts
http://dhs.gov/see-something-say-something

Exercise Only

If You See Something, Say Something™. Report suspicious activity to local law enforcement or call 911.

The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department of Homeland Security. More information is available at: www.dhs.gov/alerts. To receive mobile updates: www.twitter.com/NTASAlerts

If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

This page is intentionally left blank.

APPENDIX B: EXERCISE PARTICIPANTS

Participating Private Sector Organizations
[Insert private sector participants]

Participating Local Organizations
[Insert local participants]

Participating State Organizations
[Insert state participants]

Participating Federal Organizations
[Insert federal participants]

Other Participating Organizations
[Insert other participants]

Other Participating Organizations

This page is intentionally left blank.

APPENDIX C: RELEVANT PLANS

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

APPENDIX D: ACRONYMS

Acronym	Term
AAR	After-Action Report
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
CISA	Cybersecurity and Infrastructure Security Agency
CTEP	CISA Tabletop Exercise Package
EMS	Emergency Medical Services
EOC	Emergency Operations Center
EPT	Exercise Planning Team
FBI	Federal Bureau of Investigation
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
IED	Improvised Explosive Device
IP	Improvement Plan
JIC	Joint Information Center
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NTAS	National Terrorism Advisory System
POC	Point of Contact
PSA	Protective Security Advisor
SitMan	Situation Manual
SME	Subject Matter Expert
TTX	Tabletop Exercise

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY